Title

Secure AI-Based Voice Communication with Threat Detection and Priority Classification

Introduction

Voice-based communication systems increasingly require not only strong security but also intelligent analysis to ensure safety and timely response. This project proposes a secure voice communication framework that integrates modern cryptography with machine learning-based speech enhancement and intelligent message analysis.

Objectives

- Implement secure voice transmission using X25519 key exchange and AES encryption
- Enhance decrypted voice quality using DCCRN-based machine learning models
- Detect harmful or threatening voice messages and visually flag them
- Identify and prioritize urgent messages using BERT-based NLP models
- Detect voice bullying patterns using a combined CNN–LSTM classification model
- Develop a functional Android application

System Architecture Overview

1. User records voice via Android application
2. Voice is encrypted using AES (key derived via X25519)
3. Encrypted voice is transmitted to backend server
4. Secure decryption is performed in backend
5. Decrypted voice undergoes ML-based speech enhancement (DCCRN) and speech-to-text conversion
6. Text is analyzed for harmful content (CNN + LSTM) and urgency (BERT)
7. Messages are labeled as Safe, Harmful, or Urgent
8. Enhanced voice and priority results are returned to the user

Technologies Used

Frontend: Android (Java/Kotlin)
Backend: Python (Flask/FastAPI)
Cryptography: X25519, AES-256
Speech Enhancement: DCCRN
Speech Recognition: ASR
Bullying Detection: CNN + LSTM
Urgency Detection: BERT

Scope and Constraints

The system focuses on secure voice message processing rather than real-time calling. Machine learning models operate in a backend environment after secure decryption. The project prioritizes academic feasibility and correctness.

Expected Outcome

A working Android-based prototype demonstrating encrypted voice handling, enhanced speech clarity, harmful content detection, and urgency-based prioritization.